EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	192	713/154.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/16 20:20
L4	15	726/12.ccls. and header and encrypt$ and bypass	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/09/16 20:21
S10	7	("6052786").URPN.	USPAT	OR	ON	2007/09/16 20:09

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L6	9	header and encrypt$ and bypass and (secur$ adj policy) and malfunct$	US-PGPUB	OR	ON	2007/09/16 20:26

Published before December 2003
Terms used: **encrypt header bypass**

Found **90** of **150,573**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 90 Result page: **1** 2 3 4 5 next

Relevance scale

1 Technical correspondence: on secure personal computing

Stephen T. Kent, Doug Bates
January 1980 **Communications of the ACM**, Volume 23 Issue 1
Publisher: ACM Press
Full text available: pdf(726.72 KB) Additional Information: full citation, references

2 Design and verification of secure systems

J. M. Rushby
December 1981 **ACM SIGOPS Operating Systems Review , Proceedings of the eighth ACM symposium on Operating systems principles SOSP '81**, Volume 15 Issue 5
Publisher: ACM Press
Full text available: pdf(961.76 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper reviews some of the difficulties that arise in the verification of kernelized secure systems and suggests new techniques for their resolution. It is proposed that secure systems should be conceived as distributed systems in which security is achieved partly through the physical separation of its individual components and partly through the mediation of trusted functions performed within some of those components. The purpose of a security kernel is simply to allow such ...

3 Encryption and Secure Computer Networks

Gerald J. Popek, Charles S. Kline
December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

4 Key management for encrypted broadcast

Avishai Wool
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press

Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

5 Key management for encrypted broadcast

Avishai Wool
May 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 2
Publisher: ACM Press
Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity at the set-top terminals (STT) is severely limited due to the need to withstand pirate attacks and hardware tampering. Despite this, we would like to allow the service provider to offer different packages of programs to the users. A user ...

Keywords: conditional access, pay-per-view

6 Intrusion detection and response: An empirical analysis of NATE: Network Analysis of Anomalous Traffic Events

Carol Taylor, Jim Alves-Foss
September 2002 **Proceedings of the 2002 workshop on New security paradigms NSPW '02**
Publisher: ACM Press
Full text available: pdf(899.25 KB) Additional Information: full citation, abstract, references, index terms

This paper presents results of an empirical analysis of NATE (Network Analysis of Anomalous Traffic Events), a lightweight, anomaly based intrusion detection tool. Previous work was based on the simulated Lincoln Labs data set. Here, we show that NATE can operate under the constraints of real data inconsistencies. In addition, new TCP sampling and distance methods are presented. Differences between real and simulated data are discussed in the course of the analysis.

Keywords: intrusion detection, statistics, traffic analysis

7 Enabling email confidentiality through the use of opportunistic encryption

Simson L. Garfinkel
May 2003 **Proceedings of the 2003 annual national conference on Digital government research dg.o '03**
Publisher: Digital Government Research Center
Full text available: pdf(51.35 KB) Additional Information: full citation, abstract, references

Software for encrypting email messages has been widely available for more than 15 years, but the email-using public has failed to adopt secure messaging. This failure can be explained through a combination of technical, community, and usability factors. This paper proposes a new approach to email security that employs opportunistic encryption and a security proxy to facilitate the opportunistic exchange of keys and encryption of electronic mail. While it appears that this approach offers less se ...

8 A flow-based approach to datagram security

Suvo Mittra, Thomas Y. C. Woo
October 1997 **ACM SIGCOMM Computer Communication Review , Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies,**

architectures, and protocols for computer communication SIGCOMM '97, Volume 27 Issue 4

Publisher: ACM Press

Full text available: pdf(2.04 MB) Additional Information: full citation, abstract, references, citings, index terms

Datagram services provide a simple, flexible, robust, and scalable communication abstraction; their usefulness has been well demonstrated by the success of IP, UDP, and RPC. Yet, the overwhelming majority of network security protocols that have been proposed are geared towards connection-oriented communications. The few that do cater to datagram communications tend to either rely on long term host-pair keying or impose a session-oriented (i.e., requiring connection setup) semantics.Separately, t ...

9 Internet protocol version 6 (student paper)

Gregory R. Scholz, Clint Evans, Jaime Flores, Mustafa Rahman

March 2001 **Journal of Computing Sciences in Colleges , Proceedings of the seventh annual consortium for computing in small colleges central plains conference on The journal of computing in small colleges , Proceedings of the twelfth annual CCSC South Central conference on The journal of computing in small colleges**, Volume 16 Issue 3

Publisher: Consortium for Computing Sciences in Colleges

Full text available: pdf(72.22 KB) Additional Information: full citation, abstract, references, index terms

Many students, educators, and other professionals are increasingly finding that they need to become familiar with networking protocols. While the technical details are more complex than most professionals need, an understanding of the basic uses, features, terminology, and configurations is essential for any technical decision-maker or computer professional. Because of the Internet's dominance, computer professionals need to be, at least, familiar with its basic functionality. Currently, Inte ...

10 Building reliable, high-performance communication systems from components

Xiaoming Liu, Christoph Kreitz, Robbert van Renesse, Jason Hickey, Mark Hayden, Kenneth Birman, Robert Constable

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.49 MB) Additional Information: full citation, abstract, references, citings, index terms

Although building systems from components has attractions, this approach also has problems. Can we be sure that a certain configuration of components is correct? Can it perform as well as a monolithic system? Our paper answers these questions for the Ensemble communication architecture by showing how, with help of the Nuprl formal system, configurations may be checked against specifications, and how optimized code can be synthesized from these configurations. The performance results show that we ...

11 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on

these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

12 File-system development with stackable layers

John S. Heidemann, Gerald J. Popek
February 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 1
Publisher: ACM Press

Full text available: pdf(2.16 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Filing services have experienced a number of innovations in recent years, but many of these promising ideas have failed to enter into broad use. One reason is that current filing environments present several barriers to new development. For example, file systems today typically stand alone instead of building on the work of others, and support of new filing services often requires changes that invalidate existing work. Stackable file-system design addresses these issues in severa ...

Keywords: composability, file system design, operating system structure, reuse

13 A dynamic network architecture

Sean W. O'Malley, Larry L. Peterson
May 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 2
Publisher: ACM Press

Full text available: pdf(401.43 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Network software is a critical component of any distributed system. Because of its complexity, network software is commonly layered into a hierarchy of protocols, or more generally, into a protocol graph. Typical protocol graphs—including those standardized in the ISO and TCP/IP network architectures—share three important properties; the protocol graph is simple, the nodes of the graph (protocols) encapsulate complex functionality, and the topology of the graph ...

Keywords: composibility, dynamic configuration, reuse

14 Secure personal computing in an insecure network

Dorothy E. Denning
August 1979 **Communications of the ACM**, Volume 22 Issue 8
Publisher: ACM Press

Full text available: pdf(654.64 KB) Additional Information: full citation, abstract, references, citings

A method for implementing secure personal computing in a network with one or more central facilities is proposed. The method employs a public-key encryption device and hardware keys. Each user is responsible for his own security and need not rely on the security of the central facility or the communication links. A user can safely store confidential files in the central facility or transmit confidential data to other users on the network.

Keywords: networks, personal computing, privacy, public-key encryption, security

15 Balancing performance and flexibility with hardware support for network architectures

Ilija Hadžić, Jonathan M. Smith
November 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 4
Publisher: ACM Press
Full text available: pdf(719.03 KB) Additional Information: full citation, abstract, references, index terms

The goals of performance and flexibility are often at odds in the design of network systems. The tension is common enough to justify an architectural solution, rather than a set of context-specific solutions. The Programmable Protocol Processing Pipeline (P4) design uses programmable hardware to selectively accelerate protocol processing functions. A set of field-programmable gate arrays (FPGAs) and an associated library of network processing modules implemented in hardware are augmented with so ...

Keywords: FPGA, P4, computer networking, flexibility, hardware, performance, programmable logic devices, programmable networks, protocol processing

16 Integrating security in inter-domain routing protocols

Brijesh Kumar, Jon Crowcroft
October 1993 **ACM SIGCOMM Computer Communication Review**, Volume 23 Issue 5
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, citings, index terms

Network routing protocols work in a vulnerable environment. Unless protected by appropriate security measures, their operation can be easily subverted by intruders capable of modifying, deleting or adding false information in routing updates. This paper first analyses threats to the secure operation of inter-domain routing protocols, and then proposes various counter measures to make these protocols secure against external threats.

17 A secure distributed capability based system (extended abstract)

Howard L. Johnson, John F. Koegel, Rhonda M. Koegel
October 1985 **Proceedings of the 1985 ACM annual conference on The range of computing : mid-80's perspective: mid-80's perspective ACM '85**
Publisher: ACM Press
Full text available: pdf(1.22 MB) Additional Information: full citation, references, index terms

Keywords: capability architecture, computer security, distributed system security, network encryption

18 Distributed systems - programming and management: On remote procedure call

Patrícia Gomes Soares
November 1992 **Proceedings of the 1992 conference of the Centre for Advanced Studies on Collaborative research - Volume 2 CASCON '92**
Publisher: IBM Press
Full text available: pdf(4.52 MB) Additional Information: full citation, abstract, references, citings

The Remote Procedure Call (RPC) paradigm is reviewed. The concept is described, along with the backbone structure of the mechanisms that support it. An overview of works in supporting these mechanisms is discussed. Extensions to the paradigm that have been proposed to enlarge its suitability, are studied. The main contributions of this paper are a standard view and classification of RPC mechanisms according to different perspectives, and a snapshot of the paradigm in use today and of goals for t ...

19 File servers for network-based distributed systems

Liba Svobodova
December 1984 **ACM Computing Surveys (CSUR)**, Volume 16 Issue 4
Publisher: ACM Press

Full text available: pdf(4.23 MB) Additional Information: full citation, references, citings, index terms, review

20 Security issues for wireless ATM networks

Danai Patiyoot
January 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue 1
Publisher: ACM Press

Full text available: pdf(1.75 MB) Additional Information: full citation, abstract, references, index terms

To be able to fulfil the need of user in wireless ATM, the system has to acquire features. One of the system features for the wireless ATM is functionality especially the security aspect. There is so far tittle, if not none, security consideration in the developing of wireless ATM standard. Therefore a wide range of features in security functions is in consideration. This paper tried to define the features of security in wireless ATM networks considering it features from existing fixed ATM netwo ...

Keywords: security, wireless ATM

Results 1 - 20 of 90 Result page: **1** 2 3 4 5 next